



**Homeland
Security**

Daily Open Source Infrastructure Report

09 September 2015

Top Stories

- A section of U.S. Highway 287 near Memphis, Texas, reopened September 3 after it was closed September 1 while crews cleaned up 2,640 gallons of a toxic chemical mixture that spilled from an overturned semi-truck. – *Amarillo Globe-News* (See item [10](#))
- Crews reached 31 percent containment September 8 of the 95,884-acre Rough Fire burning in California. – *KFSN 30 Fresno* (See item [15](#))
- Kaspersky Lab released an update addressing a flaw affecting certain versions of its antivirus products, while another security researcher identified several vulnerabilities in FireEye products, including a command injection and login bypass bug. – *Securityweek* (See item [24](#))
- Security researchers found that hackers were using the Neutrino Exploit Kit (EK) to inject malicious scripts into outdated Webserver software that could potentially impact 400 million users. – *SC Magazine* (See item [25](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
 - [Chemical](#)
 - [Nuclear Reactors, Materials, and Waste](#)
 - [Critical Manufacturing](#)
 - [Defense Industrial Base](#)
 - [Dams](#)
- #### **SUSTENANCE and HEALTH**
- [Food and Agriculture](#)
 - [Water and Wastewater Systems](#)
 - [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)

Energy Sector

1. *September 4, Los Angeles Times* – (California) **Southern California air board puts new restrictions on urban oil fields.** The South Coast Air Quality Management District board approved new regulations September 4 requiring as many as 240 facilities operating over 4,000 onshore oil and gas wells in Southern California to improve odor controls and promptly respond to complaints from residents. The regulations also require the operators to adopt new odor-control measures and post signs in English and Spanish with instructions on how to report complaints, among other requirements.

Source: <http://www.latimes.com/local/lanow/la-me-ln-oil-fumes-20150904-story.html>

Chemical Industry Sector

See item [**10**](#)

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

2. *September 7, Securityweek* – (National) **Fiat Chrysler recalls SUVs to prevent remote hacking.** Fiat Chrysler Automobiles issued a recall September 7 for approximately 7,810 model year 2015 Jeep Renegade vehicles equipped with 6.5 inch touchscreens due to a vulnerability in its Uconnect system that exposed the vehicle to remote cyber-attacks. Affected customers will receive a USB device containing software updates, as well as additional security features.

Source: <http://www.securityweek.com/fiat-chrysler-recalls-suvs-prevent-remote-hacking>

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

3. *September 4, Reuters* – (International) **Credit Suisse to pay \$288 million in damages in Lake Las Vegas refinancing.** Credit Suisse Group AG was ordered to pay \$287.5 million in damages by a Texas district court to an affiliate of Highland Capital Management following an event in which the Zurich-based bank was found to have used inflated appraisals to convince the affiliate to refinance Lake Las Vegas resort in 2007. The Nevada resort community filed for Chapter 11 bankruptcy in 2008.

Source: <http://www.reuters.com/article/2015/09/05/us-credit-suisse-gp-highland-verdict-idUSKCN0R502120150905>

Transportation Systems Sector

4. *September 8, International Business Times* – (Colorado; North Carolina) **At least 7 dead in 2 place crashes in Colorado and North Carolina.** The U.S. National Transportation Safety Board reported September 8 that two separate plane crashes occurred September 6 – 7 in both Forsyth County, North Carolina, and a remote part of Colorado’s San Juan Mountains leaving a total of 7 passengers dead. An investigation is ongoing at the crash sites.
Source: <http://www.msn.com/en-us/news/us/at-least-7-dead-in-2-plane-crashes-in-colorado-and-north-carolina/ar-AAe3mUD>
5. *September 7, NBC News* – (International) **Fire sparks in Carnival Liberty cruise ship engine room.** Passengers and crew members aboard a Caribbean Carnival Cruise ship were evacuated and docked on the Island of St. Thomas September 7 while the boat’s automated fire extinguishing system doused a fire that began in one of the ship’s engine rooms. No injuries were reported and the cruise was scheduled to set sail after authorities deemed it safe.
Source: <http://www.nbcnews.com/news/us-news/fire-sparks-carnival-liberty-cruise-ship-engine-room-n423001>
6. *September 7, San Francisco Bay City News* – (California) **Accident closes SB I-880 connector to Hwy 238 in San Leandro.** California Highway Patrol issued a Sig-Alert and closed southbound Highway 880 to State Highway 238 connector in San Leandro for more than 3 hours September 7 after a vehicle struck a pole that ignited sparks and began a brush fire. Four people suffered injuries.
Source: <http://abc7news.com/traffic/accident-closes-sb-i-880-connector-to-hwy-238-in-san-leandro/972652/>
7. *September 6, KREM 2 Spokane* – (Washington) **Three woman killed in Highway 195 crash.** One northbound lane of Highway 195 near Thorpe in Spokane County reopened after all northbound lanes were closed for over 2 hours September 5 while emergency crews responded to a fatal 2-vehicle collision that killed three people and left two others injured after a vehicle failed to yield to oncoming traffic and was struck.
Source: <http://www.krem.com/story/news/local/spokane-county/2015/09/05/possible-fatal-collision-closes-highway-195-near-thorp/71786044/>
8. *September 5, Associated Press* – (Nevada) **2 dead, 4 injured after bus catches fire in Las Vegas.** Police are investigating after two people were killed and four others were injured September 5 after a fire left a mini bus as a total loss following a collision at an intersection in Las Vegas.
Source: <http://www.foxnews.com/us/2015/09/05/2-dead-4-injured-after-bus-caughts-fire-in-las-vegas/>
9. *September 4, WVEC 13 Hampton* – (Virginia) **Emergency landing at Norfolk airport.** A Southwest Airlines flight from Rhode Island’s T.F. Green Airport to Orlando International Airport made an emergency landing at Norfolk International Airport in Virginia September 4 after a smoke indicator in the aft lavatory went off. No injuries

were reported and the Federal Aviation Administration is investigating the incident.
Source: <http://www.13newsnow.com/story/news/2015/09/04/norfolk-airport-emergency-landing/71712910/>

10. **September 4, Amarillo Globe-News – (Texas) U.S. Highway 287 now open, spill cleanup continues.** A section of U.S. Highway 287 near Memphis was reopened September 3 after it was closed September 1 while crews cleaned up 2,640 gallons of a chemical mixture of lead, calcium-zinc, and Rea Tin 4435 that spilled from an overturned semi-truck.
Source: <http://amarillo.com/news/latest-news/2015-09-04/us-highway-287-reopened-spill-cleanup-continues>

Food and Agriculture Sector

11. **September 7, WQOW 18 Eau Claire – (Wisconsin) Multiple towns recover after facing flooding.** Family Farms Inc., in Eau Claire suffered over \$400,000 in damage from floods following storms that caused Strum Dam to breach September 6.
Source: <http://www.wqow.com/story/29974707/2015/09/07/dam-breach-in-strum-communities-along-buffalo-river-brace-for-flooding>
12. **September 7, WPIX 11 New York City; CNN – (International) Cucumbers recalled as deadly Salmonella outbreak affects 27 states.** Andrew & Williamson Fresh Produce issued a recall September 4 for its Limited Edition-branded cucumbers grown in Mexico, after a Salmonella Poona outbreak killed one person and sickened 285 others in 27 States. The product was sold nationally from August 1 to September 3.
Source: <http://pix11.com/2015/09/07/cucumbers-recalled-as-deadly-salmonella-outbreak-affects-27-states/>
13. **September 4, U.S. Food and Drug Administration – (New York) Food Nation issues alert on undeclared sulfites in “Western Beef packaged of Sun Dried Tomatoes.”** The U.S. Food and Drug Administration reported September 4 that Ridgewood, New York-based Food Nation Produce issued a recall for its Western Beef packaged of Sun Dried Tomatoes sold in 16 ounce or 32 ounce plastic containers due to undeclared sulfites. The products were sold in Western Beef retail supermarkets in New York.
Source: <http://www.fda.gov/Safety/Recalls/ucm461375.htm>

Water and Wastewater Systems Sector

14. **September 8, Charlotte Observer – (North Carolina) Grease blockage causes sewage spill near Piper Glen in south Charlotte.** Approximately 1,060 gallons of sewage water spilled into a tributary of Four Mile Creek in south Charlotte September 7, due to a grease blockage in the sanitary sewers.
Source: <http://www.charlotteobserver.com/news/local/article34329177.html>

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

15. *September 8, KFSN 30 Fresno* – (California) **Rough Fire forces new mandatory evacuations.** Crews reached 31 percent containment September 8 of the 95,884-acre Rough Fire burning in California. The sheriff's office ordered additional mandatory evacuations while several campgrounds remained closed until further notice.
Source: <http://abc30.com/news/rough-fire-forces-new-mandatory-evacuations/973554/>
16. *September 8, WKBN 27 Youngstown* – (Ohio) **For 2nd time in 2 weeks, bomb threat closes Niles schools.** A bomb threat against the district forced the closure of all Niles City Schools in Ohio September 8. Authorities are investigating the threat.
Source: <http://wkbn.com/2015/09/08/for-2nd-time-in-2-weeks-bomb-threat-closes-niles-schools/>
17. *September 8, KTLA 5 Los Angeles* – (California) **Classes canceled at Centennial High School in Corona due to bomb threat, ‘suspicious’ object.** A suspicious device and a bomb threat prompted the cancellation of classes at Centennial High School in Corona September 8. Police and a bomb squad responded to the scene to investigate.
Source: <http://ktla.com/2015/09/08/bomb-threat-at-centennial-high-school-in-corona-prompts-classes-to-be-canceled/>
18. *September 7, KFOR 4 Oklahoma City* – (Oklahoma) **Edmond North classes canceled due to water main break.** A September 5 water main break forced the closure of Edmond North High School in Oklahoma September 8 after 20 classrooms, the cafeteria, kitchen, and several hallways were flooded. Officials worked to clean up the damage and determine if crews are able to repair the broken water main.
Source: <http://kfor.com/2015/09/06/water-main-break-floods-part-of-edmond-north-high-school/>
19. *September 4, San Bernardino Sun* – (California) **1,600 pot plants removed from San Bernardino National Forest.** Officers removed 1,632 marijuana plants from the San Bernardino National Forest in California September 3, along with trash and irrigation line from the forest. Authorities are searching for the individuals responsible for cultivating the site.
Source: <http://www.sbsun.com/general-news/20150904/1600-pot-plants-removed-from-san-bernardino-national-forest>

Emergency Services Sector

20. *September 8, WOWK 13 Huntington* – (West Virginia) **Service outage is preventing 911 calls in part of Kanawha County, WV.** About 767 Voice over Internet Protocol (VoIP) customers in Kanawha County were affected by a 9-1-1 outage September 8, with no estimated restoral time.
Source: <http://www.wowktv.com/story/29978372/service-outage-is-preventing-911-calls-in-part-of-kanawha-county-wv>
21. *September 6, Associated Press* – (South Carolina) **SC prison employees safe after**

taken hostage by inmates. Officials are investigating after inmates took two employees hostage for 6 hours September 5 at Kirkland Correctional Institution in Columbia, South Carolina.

Source: <http://wnct.com/2015/09/06/sc-prison-employees-safe-after-taken-hostage-by-inmates/>

Information Technology Sector

22. ***September 8, Help Net Security*** – (International) **Vulnerabilities in WhatsApp web affect 200 million users globally.** WhatsApp patched a vulnerability discovered by Check Point researchers that could potentially allow hackers to execute malware on the devices via sending the user a malicious vCard contact card containing an executable file ordering it to distribute ransomware, bots, remote access tools (RAT), and other types of malicious codes.
Source: <http://www.net-security.org/secworld.php?id=18828>
23. ***September 8, Securityweek*** – (International) **Webroot, Avira patch flaws in mobile security apps.** Webroot and Avira Mobile Security released separate patches addressing vulnerabilities including, a secure sockets layer (SSL) certificate vulnerability for Webroot Mobile Protection for iOS versions 1.10.316 and prior that could have allowed a man-in-the-middle (MitM) attacker to obtain usernames, passwords, and other sensitive information. Avira Mobile Security patched a vulnerability on versions 1.5.7 and prior that allowed a MitM attacker to capture login information via an HTTP POST request.
Source: <http://www.securityweek.com/webroot-avira-patch-flaws-mobile-security-apps>
24. ***September 7, Securityweek*** – (International) **Kaspersky patches critical vulnerability in antivirus products.** Kaspersky Lab released an update addressing a flaw affecting 2015 – 2016 versions of its antivirus products related to a buffer overflow vulnerability affecting the application’s default configuration that could allow a successful exploit. A security researcher identified several vulnerabilities in FireEye products, including a command injection and login bypass bug that is being addressed by FireEye officials.
Source: <http://www.securityweek.com/kaspersky-patches-critical-vulnerability-antivirus-products>
25. ***September 7, SC Magazine*** – (International) **Ransomware risk from over 140 million websites, researchers warn.** Security researchers found that hackers were using the Neutrino Exploit Kit (EK) to inject malicious scripts into outdated Webserver software that could potentially impact 400 million users that use 142 million legitimate Web sites running out of date versions of the WordPress content management system or outdated plugins.
Source: <http://www.scmagazineuk.com/ransomware-risk-from-over-140-million-websites-researcher-warns/article/437202/>
26. ***September 7, Softpedia*** – (International) **Android pornography app takes pictures of users and blackmails them for cash.** Zscaler researchers discovered an Android app dubbed Adult Player that is used as a platform to deliver ransomware to mobile device

users by secretly taking the user's picture while it loads an Android application package (APK) file where the malware code is hosted. The photograph is used inside the ransom message.

Source: <http://news.softpedia.com/news/android-pornography-app-takes-pictures-of-users-and-blackmails-them-for-cash-491128.shtml>

27. *September 5, Softpedia* – (International) **Mozilla bug tracker hacked, data about Firefox vulnerabilities stolen.** Mozilla's bug tracker, Bugzilla, forced users with access to the bug tracker's private section to change their passwords while cutting down access to the section after engineers found that the bug tracking application was compromised, and that an attacker used a privileged account to gain access to information about unpatched Firefox vulnerabilities.
- Source: <http://news.softpedia.com/news/mozilla-bug-tracker-hacked-data-about-firefox-vulnerabilities-stolen-490980.shtml>

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

Communications Sector

28. *September 4, Ukiah Daily Journal* – (California) **Cell phone, internet service down throughout Mendocino County after cable cut.** Mendocino County officials reported that cell, landline, and Internet services for customers were expected to be restored September 4 after a 15-hour outage that began September 3 when a fiber optic cable was cut near Ritech.
- Source: <http://www.dailymodemocrat.com/general-news/20150904/cell-phone-internet-service-down-throughout-mendocino-county-after-cable-cut/1>

Commercial Facilities Sector

29. *September 8, KOMO 4 Seattle* – (Washington) **Five people injured in Capitol Hill apartment fire.** Forty residents were displaced and 5 others were injured in a September 7 fire that began inside a Capitol Hill apartment building in Seattle. The cause of the fire remains under investigation.
- Source: <http://www.komonews.com/news/local/Several-people-injured-in-Capitol-Hill-apartment-fire-325518701.html>

30. *September 7, WIBW 13 Topeka* – (Kansas) **City crews work to repair water main breaks along Wanamaker Rd, hope to prevent future breaks.** Ten businesses were without power and forced to close September 7 due to two water main breaks in Topeka, Kansas, which prompted crews to shut off water valves in surrounding areas. Water service was scheduled to be restored September 8.
- Source: <http://www.wibw.com/home/headlines/Wanamaker-water-main-break-shuts->

[businesses-325437941.html](#)

31. *September 7, KTXL 40 Sacramento* – (California) **Fair Oaks apartment fire caused by unattended barbecue.** Dozens of residents from the Village at Fair Oaks apartment complex in Fair Oaks, California, were displaced after a September 6 fire caused by an unattended barbecue that damaged or destroyed 12 units and caused more than \$400,000 worth of damages. Authorities are investigating the incident.
Source: <http://fox40.com/2015/09/07/fair-oaks-apartment-fire-caused-by-unattended-barbecue/>

Dams Sector

See item [11](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

- | | |
|-------------------------------------|---|
| Content and Suggestions: | Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590 |
| Subscribe to the Distribution List: | Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes . |
| Removal from Distribution List: | Send mail to support@govdelivery.com . |

Contact DHS

- To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
- To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.